UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,228	11/26/2003	Marco Sasselli	3829-020-27	9959

24510 7590 12/18/2007
DLA PIPER US LLP
ATTN: PATENT GROUP
500 8th Street, NW
WASHINGTON, DC 20004-2131

EXAMINER
REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/721,228	**Applicant(s)** SASSELLI ET AL.	
	Examiner Mohammad W. Reza	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This is in response to the RCE filed on 09/19/2007.

2. Claims 1-18 are pending in the application.

3. Claims 1-18 have been rejected.

Continued Examination Under 37 CFR 1.114

4. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09/19/2007 has been entered.

Response to Amendment

5. The examiner approves the amendments made to claim 1, 15.

Claim Objections

6. Claim 3 objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim which can not depend on the multiple depended claims. See MPEP § 608.01(n). Accordingly, the claim has not been further treated on the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 1-18 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. All these claims has the limitations either " repeating steps a-g for a subsequent patch data and encrypted control block using a subsequent public key selected by the apparatus from the list of public keys stored in the non-volatile memory, the subsequent public key being different from the current public key deactivated in step (g)". Examiner found in the specification in favor of this amended part but which does not discloses the limitation as presented in the claim, "The following messages M2, M3 and M4 are used to consecutively deactivate the public keys K2, K3, and K4 that correspond to each intermediate version from version 2 to version 4 preceding version 5. Therefore, to install version 5 in the non-volatile Flash memory, each public key K2, K3, and K4 of the list is used then neutralized or deleted. During the decryption of the message by the correct key, the content of this message is recognized and induces the neutralization

operation of the current key. If the message is not recognized, this means that the encryption key of this message is not the current key. After the successive and correct decryption of the messages M2, M3, M4, the key K5 necessary for the decryption of the signature of the patch (H(P))PK5 (and of patch P) becomes the current key. The latter will also be deleted from the list after the installation of the patch and the key K6 will be present at the head of list for the subsequent update of version 5 to version 6 (paragraphs, 0042-0043)".

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.
>
> When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare In re Lowry, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) and Warmerdam, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory

> product-by-process claim) with Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory).
>
> In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See Lowry, 32 F.3d at 1583-84, 32 USPQ2d at 1035.

8. Claims 9, and 10 are rejected under 35 U.S.C. 101 because the claim invention is directed to non-statutory subject matter. According to the specification of the invention (Page 1-14) **"software of an apparatus", "old version", "new version", "number message", "initial version" and "final version"** is reasonably interpreted by one of ordinary skill as just software, it is a system of software, per se. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory). Such claimed data structures do not define any structural and functional interrelationships between the data structure and other claimed aspects of the invention which permit the data structure's functionality to be realized. Similarly, computer programs claimed as computer instructions per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. Accordingly, it is important to distinguish claims that define descriptive material per se from claims that define statutory inventions. So, it does not appear that a claim reciting software with functional descriptive material falls within any of the categories of patentable subject matter set forth in § 101.

Response to Arguments

9. Applicant's arguments filed on 09/19/2007 have been fully considered but they are not persuasive.

Applicant argues that the limitations, "repeating steps a-g for a subsequent patch data and encrypted control block using a subsequent public key selected by the apparatus from the list of public keys stored in the non-volatile memory, the subsequent public key being different from the current public key deactivated in step (g)" does not disclose by Sutton or Bantz individually or in combination. However, examiner found that their combine teachings actually disclose this limitation. If a person with ordinary skill in the art would interpret this limitation then it is meaningful that this limitation is just repeating the steps of a-g as applicant also admitted. According to the specification of the application, "The following messages M2, M3 and M4 are used to consecutively deactivate the public keys K2, K3, and K4 that correspond to each intermediate version from version 2 to version 4 preceding version 5. Therefore, to install version 5 in the non-volatile Flash memory, each public key K2, K3, and K4 of the list is used then neutralized or deleted. During the decryption of the message by the correct key, the content of this message is recognized and induces the neutralization operation of the current key. If the message is not recognized, this means that the encryption key of this message is not the current key. After the successive and correct decryption of the messages M2, M3, M4, the key K5 necessary for the decryption of the signature of the patch (H(P))PK5 (and of patch P) becomes the current key. The latter will also be deleted from the list after the installation of the patch and the key K6 will be present at the head of list for the subsequent update of version 5 to version 6 (paragraphs, 0042-0043)". As Sutton discloses the subsequent patch data and encrypted control block (hash function of the digital signature) is decoded by using the key (paragraph, 0022, 0025 (last 4 lines), 0028, 0035). He also discloses that these keys are being stored in the memory (paragraph 0020). Bantz discloses the subsequent keys are different from the current public key deactivated in step (g) (it is just repeating to decode the sequence of data (col. 3, lines 30-44, and col. 4). Applicant misinterpreted that these keys are only store in the volatile memory. However, Bantz actually discloses that it could be stored in any suitable type of memory (col. 3, lines 1-2). So, considering the combine teachings of Sutton and Bantz it is reasonable that the latest amendment does not qualify the claims limitations in place for allowance.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over James A. Sutton hereafter Sutton (Patent publication 20030196096) in view of Bantz et al hereafter Bantz (US Patent 7174017).

11. As per claim 1, Sutton discloses a method comprising the steps of: selecting by means of the apparatus key from a list of public keys stored in a non-volatile memory of the apparatus (paragraphs, 0021, 0027), receiving and storing in the patch in a random access memory; receiving the encrypted control block decrypting the encrypted control block using the selected public key, verifying that the decrypted control block corresponds to said patch data, installing the patch data (paragraphs, 0013-0014, 0026), repeating steps a-g for a subsequent patch data and encrypted control block using a public key selected by the apparatus from the list of public keys stored in the non-volatile memory (paragraph, 0022, 0025 (last 4 lines), 0028, 0035). Although, Sutton discloses a particular public key used for decryption (paragraphs, 0013-0014, 0021) and different patches need different keys to decrypt the patch data (paragraphs, 0025), he does not explicitly disclose the public key is the current public key, and deactivating the current public key such that a different public key is used to decrypt a next control block, the subsequent key being different from the current key deactivated in step (g). Nevertheless, it is well known in the network security art at the time of invention that different keys require to decrypt different patch data is explaining the technology of deactivating the current decrypting key and use the new key for decrypting the new patch data. Exemplary of this is Bantz who discloses deactivating

the current public key such that a different public key is used to decrypt a next control block (col. 3, lines 30-37), the subsequent key being different from the current key deactivated in step (g) (col. 3, lines 30-37)..

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Bantz's teachings of decrypting system for encrypting audio with the teachings of Sutton, for the purpose of suitably using the new decrypting key for decrypting the patch data properly (col. 2-4).

12. As per claim 2, Sutton discloses the Method wherein the control block includes a signature on the patch data, this signature being the result of a hash function (paragraphs, 0013-0014, and 0026).

13. As per claim 3, Sutton discloses the method wherein the verification of the block includes the step of establishing the signature on the received patch and the comparison with the decrypted signature in the control block (paragraphs, 0030-0031).

14. As per claim 4, Sutton discloses the method wherein the control block includes a symmetrical session key determined by the managing center, this key being used to encrypt the patch data (paragraphs, 0021, 0027).

15. As per claim 5-7, Sutton discloses the method wherein, for each update, a new public key taken from the list is used by the apparatus, wherein the public key is deleted from the list after being used, said key being useless for the next updates, and wherein the public keys of the list are used sequentially in a predetermined order during each update (paragraphs, 0021, 0027).

16. As per claim 8, Sutton discloses the method wherein the list of public keys is stored in a non-volatile memory, a key used for an update is definitively deleted from the memory that authorizes the access to the next key for the subsequent update (paragraphs, 0014).

17. As per claim 9, Sutton discloses the method wherein, for the updating of the software of an apparatus of a an old version to a new version, with a difference between the new version and the old version being greater than one, at least one message encrypted with a private key is added allowing the changing of the current key to the next key in the list, the successful decryption of said message inducing the deactivation of the current key and the selection of the next key (paragraphs, 0021, 0027).

18. As per claim 10, Sutton discloses the method wherein the number of messages corresponds to the number of updates separating the initial version of the apparatus and the final version of the update (paragraphs, 0013-0014, and 0026).

19. As per claim 11, Sutton discloses the method wherein an updating installation is followed by an increment on a counter or by moving a pointer indicating the position of the key to be selected from the list during the subsequent update, while the list of keys remains unchanged (paragraphs, 0021, 0027).

21. As per claim 12, Sutton discloses the method according, wherein the control block is successively encrypted by the keys of the previous updates, each key from the list being used one after the other to decrypt the signature (paragraphs, 0030-0031).

22. As per claim 13, Sutton discloses the method wherein the apparatuses consist of Pay-TV decoders, an update of a decoder being carried out by downloading, from a

managing center, of a patch accompanied by a control block, said block is stored in a Random Access Memory, and is decrypted with a current public key contained in a first non-volatile memory of the decoder, then verified and in the case of correspondence, a command leads the installation of the patch in a second non-volatile memory and the deactivation of the current key (paragraphs, 0021, 0027).

23. As per claim 14, Sutton discloses the method wherein a new list of public keys is transmitted to the decoder, said list replaces the list contained in the first memory containing keys deactivated by previous successful updates (paragraphs, 0021, 0027).

24. As per claim 15, Sutton discloses a system comprising: a processor; and a non-volatile memory connected to the processor for storing a list of public keys (paragraphs, 0021, 0027); wherein the processor is configured to perform the steps of receiving the patch data; receiving an encrypted control block associated with the patch data, the encrypted control block being encrypted with an asymmetrical private key selected from a list of keys in a management center; selecting a public key from the list of public keys stored in the non-volatile memory; decrypting the encrypted control block using the key selected in the previous step; verifying that the control block corresponds to the patch data; installing the patch data if the encrypted control block corresponds to the patch data stored and key stored in the non-volatile memory (paragraphs, 0013-0014, 0026), repeating steps a-g for a subsequent patch data and encrypted control block using a public key selected by the apparatus from the list of public keys stored in the non-volatile memory (paragraph, 0022, 0025 (last 4 lines), 0028, 0035). Although, Sutton discloses a particular public key used for decryption (paragraphs, 0013-0014, 0021) and

different patches need different keys to decrypt the patch data (paragraphs, 0025), he does not explicitly disclose the public key is the current public key, and deactivating the current public key such that a different public key is used to decrypt a next control block, and the subsequent key being different from the current key deactivated in step (g). Nevertheless, it is well known in the network security art at the time of invention that different keys require to decrypt different patch data is explaining the technology of deactivating the current decrypting key and use the new key for decrypting the new patch data. Exemplary of this is Bantz who discloses deactivating the public key used in the decrypting step such that a new public key from the list of public keys (col. 3, lines 30-37), and the subsequent key being different from the current key deactivated in step (g) (col. 3, lines 30-37).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 15.

25. As per claim 16-18, Sutton discloses the system wherein the memory is an electrically erasable programmable read only memory (EEPROM), wherein the control block includes a signature on the patch data, the signature being a result of a hash function, wherein the control block includes a symmetrical session key determined by the managing center, the symmetrical session key being used to encrypt the patch data (paragraphs, 0013-0014, 0026).

Conclusion

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12/17/07